Computer Security

Web Security / 19. Same-Origin Policy

19. Same-Origin Policy

Browsing multiple webpages poses a security risk. For example, if you have a malicious website (`www.evil.com`) and Gmail (`www.gmail.com`) open, you don’t want the malicious website to be able to access any sensitive emails or send malicious emails with your identity.

Modern web browsers defend against these attacks by enforcing the same-origin policy, which isolates every webpage in your browser, except for when two webpages have the same origin.

19.1. Origins

The origin of a webpage is determined by its protocol, domain name, and port. For example, the following URL has protocol `http`, domain name `www.example.com`, and port `80`.

`http://www.example.com/index.html`

To check if two webpages have the same origin, the same-origin policy performs string matching on the protocol, domain, and port. Two websites have the same origin if their protocols, domains, and ports all exactly match.

Some examples of the same origin policy:

- `http://wikipedia.org/a/` and `http://wikipedia.org/b/` have the same origin. The protocol (`http`), domain (`wikipedia.org`), and port (none), all match. Note that the paths are not checked in the same-origin policy.
- `http://wikipedia.org` and `http://www.wikipedia.org` do not have the same origin, because the domains (`wikipedia.org` and `www.wikipedia.org`) are different.
- `http://wikipedia.org` and `https://wikipedia.org` do not have the same origin, because the protocols (`http` and `https`) are different.
- `http://wikipedia.org:81` and `http://wikipedia.org:82` do not have the same origin, because the ports (`81` and `82`) are different.

If a port is not specified, the port defaults to 80 for http and 443 for https. This means `http://wikipedia.org` has the same origin as `http://wikipedia.org:80`, but it does not have the same origin as `http://wikipedia.org:81`.

19.2. Exceptions

In general, the origin of a webpage is defined by its URL. However, there are a few exceptions to this rule:

- JavaScript runs with the origin of the page that loads it. For example, if you include `<script src="http://google.com/tracking.js"></script>` on `http://cs161.org`, the script has the origin of `http://cs161.org`.
- Images have the origin of the page that it comes from. For example, if you include `<img src="http://google.com/logo.jpg">` on `http://cs161.org`, the image has the origin of `http://google.com`. The page that loads the image (`http://cs161.org`) only knows about the image's dimensions when loading it.
- Frames have the origin of the URL where the frame is retrieved from, not the origin of the website that loads it. For example, if you include `<iframe src="http://google.com"></iframe>` on `http://cs161.org`, the frame has the origin of `http://google.com`.

JavaScript has a special function, `postMessage`, that allows webpages from different origins to communicate with each other. However, this function only allows very limited functionality.

Further reading: Same-origin policy